Intelligence Issues for Congress

Richard A. Best Jr.
Specialist in National Defense

March 3, 2011

Congressional Research Service
7-5700
www.crs.gov
RL33539

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

To address the challenges facing the U.S. intelligence community in the 21st century, congressional and executive branch initiatives have sought to improve coordination among the different agencies and to encourage better analysis. In December 2004, the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) was signed, providing for a Director of National Intelligence (DNI) with substantial authorities to manage the national intelligence effort. The legislation also established a separate Director of the Central Intelligence Agency.

Making cooperation effective presents substantial leadership and managerial challenges. The needs of intelligence "consumers"—ranging from the White House to Cabinet agencies to military commanders—must all be met, using the same systems and personnel. Intelligence collection systems are expensive and some critics suggest there have been elements of waste and unneeded duplication of effort while some intelligence "targets" have been neglected.

The DNI has substantial statutory authorities to address these issues, but the organizational relationships remain complex, especially for intelligence agencies that are part of the Defense Department. Members of Congress will be seeking to observe the extent to which effective coordination is accomplished.

International terrorism, a major threat facing the United States in the 21st century, presents a difficult analytical challenge, vividly demonstrated by the attempted bombing of a commercial aircraft approaching Detroit on December 25, 2009. Counterterrorism requires the close coordination of intelligence and law enforcement agencies, but there remain many institutional and procedural issues that complicate cooperation between the two sets of agencies. Particular challenges relate to the protection of civil liberties that surround collecting information about U.S. persons.

Techniques for acquiring and analyzing information on small groups of plotters differ significantly from those used to evaluate the military capabilities of other countries, with a much higher need for situational awareness of third world societies. U.S. intelligence efforts are complicated by unfilled requirements for foreign language expertise.

Intelligence on Iraqi weapons of mass destruction was inaccurate and Members have criticized the performance of the intelligence community in regard to current conditions in Afghanistan, Iran, and other areas. Improved analysis, while difficult to mandate, remains a key goal. Better human intelligence, it is widely agreed, is also essential, but very challenging to acquire.

Intelligence support to military operations continues to be a major responsibility of intelligence agencies. The use of precision guided munitions depends on accurate, real-time targeting data; integrating intelligence data into military operations challenges traditional organizational relationships and requires innovative technological approaches.

Contents

Contacts

Most Recent Developments

On February 25, President Obama signed H.R. 514 (P.L. 112-3) to extend expiring provisions of the USA Patriot Act and the Intelligence Reform Act dealing with business records, individual terrorists as agents of foreign powers, and roving wiretaps until May 27. Earlier proposals to extend them for longer periods were unsuccessful. During a public hearing on February 10, Representative Rogers, chairman of the House Permanent Select Committee on Intelligence, highlighted major concerns for the committee based on a need to take stock of developments since 2001. He specifically mentioned the need to extend USA PATRIOT Act provisions that expire in 2011, to reexamine the Communications Enforcement for Law Enforcement Act (CALEA), and legal authorities concerning detainees. Also mentioned was an intention to review the performance of institutions established since 9/11—the Office of the Director of National Intelligence, the National Counterterrorism Center, and the intelligence offices of the FBI. Representative Ruppersberger, the ranking Member, emphasized the need the need to address cybersecurity issues and the high costs of the space reconnaissance program

Background and Analysis

The attacks on the World Trade Center and the Pentagon on September 11, 2001, dramatically demonstrated the intelligence threats facing the United States in the new century. In response, Congress approved significantly larger intelligence budgets and, in December 2004, passed the most extensive reorganization of the intelligence community since the National Security Act of 1947. The Intelligence Reform and Terrorism Prevention Act of 2004 (hereinafter, the "Intelligence Reform Act") (P.L. 108-458) created a Director of National Intelligence (separate from a Director of the Central Intelligence Agency) who heads the intelligence community, serves as the principal intelligence adviser to the President, and oversees and directs the acquisition of major collections systems. As long urged by some outside observers, one individual is now charged with concentrating on the intelligence community as a whole and possesses statutory authorities for establishing priorities for budgets, for directing collection by the whole range of technical systems and human agents, and for the preparation of community-wide analytical products.

P.L. 108-458 was designed to address the findings of the National Commission on Terrorist Attacks Upon the United States, known as the 9/11 Commission, that there has been inadequate coordination of the national intelligence effort and that the intelligence community, as then-organized, could not serve as an agile information gathering network in the struggle against international terrorists. The commission released its report in late July 2004, and Congress debated its recommendations through the following months. A key issue was the extent of the authorities of the DNI, especially with regard to budgeting for technical collection systems managed by Defense Department agencies. In the end, many of the recommendations of the 9/11 Commission regarding intelligence organization were adopted after a compromise provision was included that called for implementing the act "in a manner that respects and does not abrogate" the statutory authorities of department heads.

On April 21, 2005, the Senate confirmed the nominations of John D. Negroponte, who had served as Ambassador to Iraq, as DNI and Lt. General Michael V. Hayden, then Director of the National Security Agency, as Deputy DNI. (In May 2006 Hayden became Director of the CIA.) On February 7, 2007, retired Navy Vice Admiral J. Michael McConnell was confirmed by the Senate

as Negroponte's successor as DNI. Retired Admiral Dennis C. Blair was confirmed as the third DNI on January 28. Blair resigned in May 2010 and retired Air Force Lt. General James R. Clapper, Jr. became the fourth DNI in August 2010. Leon C. Panetta, former House Member and Director of the Office of Management and Budget under President Clinton, was confirmed as CIA Director on February 12, 2009.

Intelligence Community

The intelligence community (defined at 50 U.S.C. 401a(4)) consists of the following:

Central Intelligence Agency (CIA)

Bureau of Intelligence and Research, Department of State (INR)

Defense Intelligence Agency (DIA)

National Security Agency (NSA)

National Reconnaissance Office (NRO)

National Geospatial-Intelligence Agency (NGA)

Federal Bureau of Investigation (FBI)

Army Intelligence

Navy Intelligence

Air Force Intelligence

Marine Corps Intelligence

Department of Homeland Security (DHS)

Coast Guard (CG)

Treasury Department

Energy Department

Drug Enforcement Agency (DEA)

Except for the CIA, intelligence offices or agencies are components of Cabinet departments with other roles and missions. The intelligence offices/agencies, however, participate in intelligence community activities while supporting the other efforts of their departments.

The CIA remains the keystone of the intelligence community. It has all-source analytical capabilities that cover the whole world outside U.S. borders. It produces a range of studies that address virtually any topic of interest to national security policymakers. The CIA also collects intelligence with human sources and, on occasion, undertakes covert actions at the direction of the President. (A covert action is an activity or activities of the U.S. government to influence

political, economic, or military conditions abroad, where it is intended that the U.S. role will not be apparent or acknowledged publicly.)

Three major national-level intelligence agencies in DOD—the National Security Agency (NSA), the National Reconnaissance Office (NRO), and the National Geospatial-Intelligence Agency (NGA)—absorb the larger part of the national intelligence budget. NSA is responsible for signals intelligence and has collection sites throughout the world. The NRO develops and operates reconnaissance satellites. The NGA prepares the geospatial data—ranging from maps and charts to sophisticated computerized databases—necessary for targeting in an era in which military operations are dependent upon precision-guided weapons. In addition to these three agencies, the Defense Intelligence Agency (DIA) is responsible for defense attachés and for providing DOD with a variety of analytical products. Although the Intelligence Reform Act provides extensive budgetary and management authorities over these agencies to the DNI, it does not revoke the responsibilities of the Secretary of Defense for these agencies.

The State Department's Bureau of Intelligence and Research (INR) is one of the smaller components of the intelligence community but is widely recognized for the high quality of its analysis. INR is strictly an analytical agency; diplomatic reporting from embassies, though highly useful to intelligence analysts, is not considered an intelligence function (nor is it budgeted as one).

The key intelligence functions of the FBI relate to counterterrorism and counterintelligence. The former mission has grown enormously in importance since September 2001, many new analysts have been hired, and the FBI has been reorganized in an attempt to ensure that intelligence functions are not subordinated to traditional law enforcement efforts. Most importantly, law enforcement information is now expected to be forwarded to other intelligence agencies for use in all-source products.

The intelligence organizations of the four military services concentrate largely on concerns related to their specific missions. Their analytical products, along with those of DIA, supplement the work of CIA analysts and provide greater depth on key military and technical issues.

The Homeland Security Act (P.L. 107-296) provided the new Department of Homeland Security (DHS) responsibilities for fusing law enforcement and intelligence information relating to terrorist threats to the homeland. The Office of Intelligence and Analysis in DHS participates in the inter-agency counterterrorism efforts and, along with the FBI, has focused on ensuring that state and local law enforcement officials receive information on terrorist threats from national-level intelligence agencies.

The Coast Guard, now part of DHS, deals with information relating to maritime security and homeland defense. The Energy Department analyzes foreign nuclear weapons programs as well as nuclear nonproliferation and energy-security issues. It also has a robust counterintelligence effort. The Treasury Department collects and processes information that may affect U.S. fiscal and monetary policies. Treasury also covers the terrorist financing issue.

Authorization Legislation

Annual intelligence authorization bills were enacted from FY1979 through FY2005, providing congressional authorization for intelligence programs and guidance to the several intelligence agencies in specific provisions and report language. No intelligence authorization legislation was

enacted between December 2004 and October 2010. On September 16, 2009, the Senate approved an amended version of the FY2010 Intelligence Authorization bill (S. 1494) on voice vote. The bill would require Senate confirmation of future nominees to head the NSA, the NRO, and the NGA, and to serve as deputy director of the CIA. It would also strengthen the role of the DNI in managing acquisitions of intelligence systems. The two intelligence committees are to be kept informed of all covert actions and other intelligence activities; if the executive branch intends not to inform all Members of the committees, the committees are to be advised of the "main features" of the activity in a form that could be accessible to all committee Members. In a provision that has been under consideration for some years, the bill would establish a statutory Inspector General for the entire intelligence community. It would also require that the Administration disclose the amount requested in the annual budget for the National Intelligence Program. At the request of the Administration, the Senate Intelligence Committee separated issues of terrorist detention and interrogation from the bill and indicated an intention to address these issues in separate legislation. Differences over these issues had contributed to the inability to enact intelligence authorization legislation since 2004. Although details of satellite programs are contained in the classified annex to the accompanying report (S.Rept. 111-55), the legislation recommends "a more capable and more affordable imagery architecture" than currently exists with some observers suggesting that provisions in S. 1494 differ significantly from provisions in the defense appropriations bill that was subsequently enacted as P.L. 111-118.

On June 26, 2009, the House Intelligence Committee reported (H.Rept. 111-186) its version of the FY2010 Intelligence Authorization Act, H.R. 2701. If enacted, the legislation would have curtailed implementation of the Defense Civilian Intelligence Personnel System, required that the President brief Members of the intelligence committees on both planned intelligence activities and covert actions unless he certified the need to limit notification for "extraordinary circumstances." The bill would also have required that the Senate confirm nominees to head the NRO and NSA (but not the NGA); the bill would establish the position of deputy director of the CIA to be appointed by the President but does not require Senate confirmation for filling this position. The bill would also have established a statutory Inspector General for the intelligence community. The Administration criticized several provisions in the bill as originally reported and threatened a veto of provisions that would alter current law that permits notification of covert actions to only the "Gang of Eight," rather than the full membership of the two intelligence committees. H.R. 2701 did not receive floor consideration in the House until late February 2010 when the legislation was passed with amendments intended to meet the Administration's concerns about excessive restrictions on covert action notifications. Media reports in mid-May 2010 indicated that informal discussions with the Administration had prepared the way for conference. The June 2010 version of H.R. 2701 would require covert action notifications that are made to a limited number of Members to be based on a certification "that it is essential to limit access ... to meet extraordinary circumstances affecting vital interests of the United States." The certification would have to be reviewed within 180 days.

After extensive negotiations with the Obama Administration, the Senate passed a new version of H.R. 2701 on September 27, 2010, based largely on S. 3611 that had passed the Senate earlier. Inasmuch as FY2010 was nearing its end, the final version of H.R. 2701 did not include a classified annex specifying funding levels for intelligence programs. The bill did include provisions to require that in the case of findings regarding covert actions that are not made available to all Members of the two intelligence committees, the President shall within 180 days advise all committee Members that a finding has been forwarded to key congressional leaders (the "Gang of Eight"). In addition, the President is to provide to all Members a "general description" of the finding.

The version of H.R. 2701 passed in September 2010 would also establish the position of Inspector General of the Intelligence Community within the Office of the DNI and giving the incumbent broad responsibilities in regard to all intelligence agencies. The legislation provides the DNI with authority to undertake accountability reviews throughout the intelligence community and gives him enhanced statutory authorities in regard to acquisition programs. The position of Deputy Director of the CIA is established but without a requirement for Senate confirmation. As discussed below the DNI is required to prepare a directive governing access to intelligence information by the General Accountability Office.

Also included are several initiatives to support foreign language training, including one with special focus on African languages. H.R. 2701 also establishes a Commission on Foreign Intelligence and Information within the legislative branch. The bill was signed by President Obama on October 7, 2010, and became P.L. 111-259.

The "INTs": Intelligence Disciplines

The intelligence community has been built around major agencies responsible for specific intelligence collection systems known as disciplines. Three major intelligence disciplines or "INTs"—signals intelligence (*sigint*), imagery intelligence (*imint*), and human intelligence (*humint*)—provide the most important information for analysts and absorb the bulk of the intelligence budget. Sigint collection is the responsibility of NSA at Fort Meade, MD. Sigint operations are classified, but there is little doubt that the need for intelligence on a growing variety of nations and groups that are increasingly using sophisticated and rapidly changing encryption systems requires a far different sigint effort than the one prevailing during the Cold War. Since the late 1990s a process of change in NSA's culture and methods of operations has been initiated, a change required by the need to target terrorist groups and affected by the proliferation of communications technologies and inexpensive encryption systems. Observers credit the then-Director of NSA, Lieutenant General Michael Hayden, who later became Director of the CIA in May 2006, with launching a long-overdue reorganization of the agency, and adapting it to changed conditions. Part of his initiative has involved early retirements for some NSA personnel and greater reliance on outsourcing many functions previously done by career personnel. Some of the initiatives relating to acquisition did not, however, meet their objectives.

A second major intelligence discipline, imagery or *imint*, is also facing profound changes. Imagery is collected in essentially three ways: by satellites, manned aircraft, and unmanned aerial vehicles (UAVs). The satellite program that covered the Soviet Union and acquired highly accurate intelligence concerning submarines, missiles, bombers, and other military targets is perhaps the greatest achievement of the U.S. intelligence community—it served as a foundation for defense planning and strategic planning that led to the end of the Cold War. In today's environment, there is a greater number of collection targets than existed during the Cold War and more satellites are required, especially those that can be maneuvered to collect information about a variety of targets. At the same time, the availability of high-quality commercial satellite imagery and its widespread use by federal agencies has raised questions about the extent to which coverage from the private sector can meet the requirements of intelligence agencies. High altitude UAVs such as the Global Hawk may also provide surveillance capabilities that overlap those of satellites.

The National Imagery and Mapping Agency (NIMA) was established in 1996 to manage imagery processing and dissemination previously undertaken by a number of separate agencies. NIMA was renamed the National Geospatial-Intelligence Agency (NGA) by the FY2004 Defense

Authorization Act (P.L. 108-136). The goal of NGA is, according to the agency, to use imagery and other geospatial information "to describe, assess, and visually depict physical features and geographically referenced activities on the Earth."

Intelligence from human contacts—*humint*—is the oldest intelligence discipline and the one that is most often written about in the media. The CIA is the primary collector of humint, but the Defense Department also has responsibilities filled by defense attachés at embassies around the world and by other agents working on behalf of theater commanders. Many observers have argued that inadequate humint has been a systemic problem and contributed to the inability to gain prior knowledge of the 9/11 plots. In part, these criticisms reflect the changing nature of the international environment. During the Cold War, principal targets of U.S. humint collection were foreign government officials and military leaders. Intelligence agency officials working under cover as diplomats could approach potential contacts at receptions or in the context of routine embassy business. Today, however, the need is to seek information from clandestine terrorist groups or narcotics traffickers who do not appear at embassy social gatherings. Humint from such sources can be especially important as there may be little evidence of activities or intentions that can be gathered from imagery, and their communications may be carefully limited.

Placing U.S. intelligence officials in foreign countries under "nonofficial cover" (NOC) in businesses or other private capacities is possible, but it presents significant challenges to U.S. agencies. Administrative mechanisms are vastly more complicated than they are for officials formally attached to an embassy; special arrangements have to be made for pay, allowances, retirement, and healthcare. The responsibilities of operatives under nonofficial cover to the parent intelligence agency have to be reconciled with those to private employers, and there is an unavoidable potential for conflicts of interest or even corruption. Any involvement with terrorist groups or smugglers has a potential for major embarrassment to the U.S. government and, of course, physical danger to those immediately involved.

Responding to allegations that CIA agents may have been involved too closely with narcotics smugglers and human rights violators in Central America, the then-Director of Central Intelligence (DCI), John Deutch, established guidelines in 1995 (which remain classified) to govern the recruitment of informants with unsavory backgrounds. Although CIA officials maintain that no proposal for contacts with persons having potentially valuable information was disapproved, there was a widespread belief that the guidelines served to encourage a "risk averse" atmosphere at a time when information on terrorist plans, from whatever source, was urgently sought. The FY2002 Intelligence Authorization Act (P.L. 107-108) directed the DCI to rescind and replace the guidelines, and July 2002 press reports indicated that they had been replaced.

A major constraint on humint collection is the availability of personnel trained in appropriate languages. Cold war efforts required a supply of linguists in a relatively finite set of foreign languages, but the intelligence community now needs experts in a wider range of more obscure languages and dialects. Various approaches have been considered: use of civilian contract personnel, military reservists with language qualifications, and substantial bonuses for agency personnel who maintain their proficiency. The National Security Education Program, established in 1991, provides scholarships and career training for individuals in or planning to enter careers in agencies dealing with national security issues.

Other "INTs"

A fourth INT, measurement and signatures analysis—*masint*—has received greater emphasis in recent years. A highly technical discipline, masint involves the application of complicated analytical refinements to information collected by sigint and imint sensors. It also includes spectral imaging by which the identities and characteristics of objects can be identified on the basis of their reflection and absorption of light. Masint is undertaken by DIA and other DOD agencies. A key problem has been retaining personnel with expertise in masint systems who are offered more remunerative positions in private industry.

Another category of information, open source information—*osint* (newspapers, periodicals, pamphlets, books, radio, television, and Internet websites)—is increasingly important given requirements for information about many regions and topics (instead of the former concentration on political and military issues affecting a few countries). At the same time, requirements for translation, dissemination, and systematic analysis have increased, given the multitude of different areas and the volume of materials. Many observers believe that intelligence agencies should be more aggressive in using osint; some believe that the availability of osint may even reduce the need for certain collection efforts. The availability of osint also raises questions regarding the need for intelligence agencies to undertake collection, analysis, and dissemination of information that could be directly obtained by user agencies. Section 1052 of the Intelligence Reform Act expressed the sense of Congress that there should be an open source intelligence center to coordinate the collection, analysis, production, and dissemination of open source intelligence to other intelligence agencies. An Open Source Center was subsequently established, although it has been managed by CIA personnel.

Integrating the "INTs"

The "INTs" have been the pillars of the intelligence community's organizational structure, but analysis of threats requires that data from all the INTs be brought together and that analysts have ready access to all sources of data on a timely basis. This has proved in the past to be a substantial challenge because of technical problems associated with transmitting data and the need to maintain the security of information acquired from highly sensitive sources. Some argue that intelligence officials have tended to err on the side of maintaining the security of information even at the cost of not sharing essential data with those having a need to know. Section 1015 of the Intelligence Reform Act mandated the establishment of an Intelligence Sharing Environment (ISE) to facilitate terrorism-related information.

A related problem has been barriers between foreign intelligence and law enforcement information. These barriers derived from the different uses of information collected by the two sets of agencies—foreign intelligence used for policymaking and military operations and law enforcement information to be used in judicial proceedings in the United States. A large part of the statutory basis for the "wall" between law enforcement and intelligence information was removed with passage of the USA PATRIOT Act of 2001 (P.L. 107-56), which made it possible to share law enforcement information with analysts in intelligence agencies, but long-established practices have not been completely overcome. The Homeland Security Act (P.L. 107-296) and the subsequent creation of the Terrorist Threat Integration Center (TTIC) established offices charged with combining information from both types of sources. Section 1021 of the Intelligence Reform Act made the new National Counterterrorism Center (NCTC), TTIC's successor, operating under the DNI specifically responsible for "analyzing and integrating all intelligence possessed or

acquired by the United States Government pertaining to terrorism and counterterrorism [except purely domestic terrorism]."[1]

Intelligence Budget Process

For budgetary purposes, intelligence spending is divided between the National Intelligence Program (NIP; formerly the National Foreign Intelligence Program or NFIP) and the Military Intelligence Program (MIP). The MIP was established in September 2005 and includes all programs from the former Joint Military Intelligence Program, which encompassed DOD-wide intelligence programs and most programs from the former Tactical Intelligence and Related Activities (TIARA) category, which encompassed intelligence programs supporting the operating units of the armed services. The Program Executive for the MIP is the Under Secretary of Defense for Intelligence. Thus far, only a small part of the intelligence budget has been made public; the bulk of the $53.1 billion in national intelligence spending has been "hidden" within the DOD budget. DCI Clapper has announced plans to take the NIP out of the DOD budget beginning in 2013. If that occurs Congress may consider separate intelligence appropriations legislation in addition to defense appropriations bills. Spending for most intelligence programs is described in classified annexes to intelligence and national defense authorization and appropriations legislation. (Members of Congress have access to these annexes, but must make special arrangements to read them.)

Intelligence spending is authorized in intelligence authorization acts. When intelligence authorization legislation has not been enacted (as has been the case since FY2005), most intelligence spending is authorized by a "catch-all" provision in defense appropriations acts.[2]

For a number of years some Members sought to make public total amounts of intelligence and intelligence-related spending; floor amendments for that purpose were defeated in both chambers during the 105th Congress. In response, however, to a lawsuit filed under the Freedom of Information Act, DCI George Tenet stated on October 15, 1997, that the aggregate amount appropriated for intelligence and intelligence-related activities for FY1997 was $26.6 billion. He added that the Administration would continue "to protect from disclosure any and all subsidiary information concerning the intelligence budget." In March 1998, DCI Tenet announced that the FY1998 figure was $26.7 billion. Figures for FY1999 and subsequent years were not been released. During consideration of intelligence reform legislation in 2004, the Senate at one point approved a version of a bill which would require publication of the amount of the NIP; the House version did not include a similar provision and, with the Senate deferring to the House, the Intelligence Reform Act did not require making intelligence spending amounts public. Section 601 of P.L. 110-53, Implementing Recommendations of the 9/11 Commission Act of 2007, requires, however, that the DNI publicly disclose the aggregate amount of funds appropriated for the NIP although after FY2008 the President could waive or postpone the disclosure upon sending a explanation to congressional oversight committees. Consistent with that act, the DNI announced in October 2008 that the aggregate amount appropriated to the National Intelligence Program for FY2008 was $47.5 billion. A year later the NIP for FY2009 was announced as $49.8

[1] See CRS Report R41022, *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*, by Richard A. Best Jr.

[2] See CRS Report R40240, *Intelligence Authorization Legislation: Status and Challenges*, by Richard A. Best Jr. The FY2010 Intelligence Authorization Act (P.L. 111-259) was not enacted prior to the end of FY2010 and did not authorized FY2010 intelligence programs although it had significant legislative provisions.

billion. In September 2009, DNI Blair stated publicly that total annual intelligence spending is $75 billion, a figure that includes not only the NIP but also military intelligence activities. In October 2010, the DNI announced that the amount appropriated to the NIP for FY2010 was $53.1 billion.

Jurisdiction over intelligence programs is somewhat different in the House and the Senate. The Senate Intelligence Committee has jurisdiction only over the NIP but not the MIP, whereas the House Intelligence Committee has jurisdiction over both sets of programs. The preponderance of intelligence spending is accomplished by intelligence agencies within DOD and thus in both chambers the armed services committees are involved in the oversight process. Other oversight committees are responsible for intelligence agencies that are part of departments over which they have jurisdiction.

Most appropriations for intelligence activities are included in national defense appropriations acts, including funds for the CIA, DIA, NSA, the NRO, and NGA. Other appropriations measures include funds for the intelligence offices of the State Department, the FBI, and DHS. In the past, defense appropriations subcommittees have funded the intelligence activities of CIA and the DOD agencies (although funds for CIA have been included in defense appropriations acts, these monies are transferred directly to the CIA Director). The Senate voted in October 2004 to establish an Appropriations Subcommittee on Intelligence, but this has not occurred nor did the House take similar action. On January 9, 2007, however, the House approved H.Res. 35, which established a select panel within the appropriations committee that includes three Members of the intelligence committee to oversee appropriations for intelligence program. Reportedly, the select panel will not be continued in the 112th Congress. Instead, it is anticipated that the need for budgetary review of intelligence programs will be met by coordination among the appropriations committees and other committees with jurisdiction over intelligence efforts.

Intelligence budgeting issues were at the center of the debate on intelligence reform legislation in 2004. On one hand, there was determination to make the new DNI responsible for developing and determining the annual National Intelligence Program budget (which is separate from the MIP budgets that are prepared by the Office of the Secretary of Defense). The goal was to ensure a unity of effort that arguably has not previously existed and that may have complicated efforts to monitor terrorist activities. On the other hand, the intelligence efforts within the National Intelligence Program include those of major components of the Defense Department, including NSA, the NRO, and NGA, that are closely related to other military activities. Some Members thus argued that even the National Intelligence Program should not be considered apart from the Defense budget. After considerable debate, the final version of P.L. 108-458 provides broad budgetary authorities to the DNI, but in Section 1018 requires the President to issue guidelines to ensure that the DNI exercises the authorities provided by the statute "in a manner that respects and does not abrogate the statutory responsibilities of the heads of" the Office of Management and Budget and Cabinet departments. Observers expect that implementing the complex and seemingly overlapping budgetary provisions of the Intelligence Reform Act will continue to depend on effective working relationships between the Office of the DNI, DOD, and the President.

The 9/11 Investigations and the Congressional Response

In the aftermath of September 11, 2001, there was extensive public discussion of whether the attacks on the Pentagon and World Trade Center represented an "intelligence failure." In response, the Senate Select Committee on Intelligence and the House Permanent Select

Committee on Intelligence undertook a joint investigation of the September 11 attacks. Public hearings by the resulting "Joint Inquiry" were launched on September 18, 2002, beginning with testimony from representatives of families of those who died in the attacks. Former policymakers and senior CIA and FBI officials also testified. Eleanor Hill, the inquiry staff director, summarized the inquiry's findings:

> the Intelligence Community did have general indications of a possible terrorist attack against the United States or U.S. interests overseas in the spring and summer of 2001 and promulgated strategic warnings. However, it does not appear that the Intelligence Community had information prior to September 11 that identified precisely where, when and how the attacks were to be carried out.

The two intelligence committees published the findings and conclusions of the Joint Inquiry on December 11, 2002.[3] The committees found that the intelligence community had received, beginning in 1998 and continuing into the summer of 2001, "a modest, but relatively steady, stream of intelligence reporting that indicated the possibility of terrorist attacks within the United States." Further findings dealt with specific terrorists about whom some information had come to the attention of U.S. officials prior to September 11 and with reports about possible employment of civilian airliners to crash into major buildings. The inquiry also made systemic findings highlighting the intelligence community's lack of preparedness to deal with the challenges of global terrorism, inefficiencies in budgetary planning, the lack of adequate numbers of linguists, a lack of human sources, and an unwillingness to share information among agencies.

Separately, the two intelligence committees submitted recommendations for strengthening intelligence capabilities. They urged the creation of a Cabinet-level position of Director of National Intelligence (DNI) separate from the position of director of the CIA. The DNI would have greater budgetary and managerial authority over intelligence agencies in the Defense Department than possessed by the DCI. The committees also expressed great concern with the reorientation of the FBI to counterterrorism and suggested consideration of the creation of a new domestic surveillance agency similar to Britain's MI5.

The Joint Inquiry was focused directly on the performance of intelligence agencies, but there was widespread support among Members for a more extensive review of the roles of other government agencies. Provisions for establishing an independent commission on the 2001 terrorist attacks were included in the FY2003 Intelligence Authorization Act (P.L. 107-306). Former New Jersey Governor Thomas H. Kean was named to serve as chairman, with former Representative Lee H. Hamilton serving as vice chairman. Widely publicized hearings were held in spring 2004 with Administration and outside witnesses providing different perspectives on the role of intelligence agencies prior to the September 11, 2001, attacks. The commission's report was published in July 2004.

Although the 9/11 Commission surveyed the roles of a number of federal and local agencies, many of its principal recommendations concerned the perceived lack of authorities of the DCI. The commission recommended establishing a National Intelligence Director (NID) to manage the National Intelligence Program and oversee the agencies that contribute to it. The NID would annually submit a national intelligence program budget and, when necessary, forward the names of nominees to be heads of major intelligence agencies to the President. Lead responsibility for conducting and executing paramilitary operations would be assigned to DOD and not CIA. The

[3] The full report was released some months later as H.Rept. 107-792/S.Rept. 107-351.

commission also recommended that Congress pass a separate annual appropriations act for intelligence that would be made public. The NID would execute the expenditure of appropriated funds and make transfers of funds or personnel as appropriate. Proposing a significant change in congressional practice, the commission recommended a single intelligence committee in each house of Congress, combining authorizing and appropriating authorities.

On August 27, 2004, President Bush addressed key recommendations of the 9/11 Commission in signing several executive orders to reform intelligence. In addition to establishing a National Counterterrorism Center, the orders provided new authorities for the DCI until legislation was enacted to create a National Intelligence Director. In addition, several legislative proposals were introduced to establish a National Intelligence Director, separate from a CIA Director. The Senate passed S. 2845 on October 16, 2004; the House had passed H.R. 10 on October 8, 2004. Efforts by the resulting conference committee to reach agreed-upon text focused on the issue of the authorities of the proposed Director of National Intelligence in regard to the budgets and operations of the major intelligence agencies in DOD, especially NSA, NRO, and NGA. Conferees finally reached agreement in early December, and the conference report on S. 2845 (H.Rept. 108-796) was approved by the House on December 7 and by the Senate on December 8. The President signed the legislation on December 17, 2004, and it became P.L. 108-458.

The Intelligence Reform Act is wide-ranging (as noted below) and its ongoing implementation will undoubtedly continue to receive oversight during the 112th Congress. Some observers have suggested that modifications to the legislation may be needed; others recommend that any difficulties be addressed by executive orders or memoranda of understanding.

Oversight Issues

The 9/11 Commission concluded that congressional oversight of intelligence activities was "dysfunctional." A number of measures were undertaken to address issues raised by the commission, including the establishment of oversight subcommittees on both intelligence committees, but proposals to establish one committee with both appropriations and authorization responsibilities proved unacceptable. Both House and Senate rules require that the respective intelligence committees include Members also serving on the Appropriations Committee, thus providing for a measure of coordination.

The involvement of the intelligence community in homeland security efforts that involve domestic law enforcement agencies has affected congressional oversight. In the past the two intelligence committees and the appropriations committees were almost the only points of contact between intelligence agencies and the Congress. In the 109th Congress the House Homeland Security Committee and the Senate Homeland Security and Governmental Affairs Committee also undertook oversight of some aspects of intelligence activities.

Ongoing Congressional Concerns

Collection Capabilities

Intelligence agencies collect vast quantities of information on a daily, even an hourly basis. The ability to locate fixed installations and moving targets has become an integral component of U.S. military capabilities. On almost any subject, the intelligence community can provide a wealth of

knowledge within short time frames. Inevitably, there are "mysteries" that remain unknowable—the effects of unforeseeable developments and the intentions of foreign leaders. The emergence of the international terrorist threat has posed major challenges to intelligence agencies largely designed to gather information about nation states and their armed forces. Sophisticated terrorist groups in some cases relay information only via agents in order to avoid having their communications intercepted. Human collection has been widely perceived as inadequate, especially in regard to terrorism; the Intelligence Reform Act stated the sense of Congress that, while humint officers have performed admirably and honorably, there must be an increased emphasis on and greater resources applied to enhancing the depth and breadth of human intelligence capabilities. In October 2005 the National Clandestine Service was established at CIA to manage humint operations by CIA and coordinate humint efforts by other intelligence agencies.

There are also congressional concerns regarding major technical systems—especially reconnaissance satellites. These programs have substantial budgetary implications. Whereas the intelligence community was a major technological innovator during the Cold War, today both intelligence agencies and their potential targets make extensive use of commercial technologies, including sophisticated encryption systems. Filtering out "chaff" from the ocean of data that can be collected remains, however, a major challenge. Consensus has yet to be reached on acquisition programs for a new generation of satellites.

Analytical Quality

The ultimate goal of intelligence is accurate analysis. Analysis is not, however, an exact science and there have been, and undoubtedly will continue to be, failures by analysts to prepare accurate and timely assessments and estimates. The performance of the intelligence community's analytical offices during the past decade is a matter of debate; some argue that overall the quality of analysis has been high while others point to the failure to provide advance warning of the 9/11 attacks and a flawed estimate of Iraqi weapons of mass destruction as reflecting systemic problems. Congressional intelligence committees have for some time noted weaknesses in analysis and lack of language skills, and a predominant focus on current intelligence at the expense of strategic analysis.

Analytical shortcomings are not readily addressed by legislation, but Congress has increased funding for analytical offices since 9/11 and the Intelligence Reform Act of 2004 contains a number of provisions designed to improve analysis—an institutionalized mechanism for alternate or "red team" analyses to be undertaken (Section 1017), the designation of an individual or entity to ensure that intelligence products are timely, objective, and independent of political considerations (Section 1019), and the designation of an official in the office of the DNI to whom analysts can turn for counsel, arbitration on "real or perceived problems of analytical tradecraft or politicization, biased reporting, or lack of objectivity" (Section 1020).

These efforts will, however, be affected by the long lead times needed to prepare and train analysts, especially in such fields as counterterrorism and counterproliferation. Improving analysis depends, among other things, upon the talents of analysts brought into government service, encouraging their contributions and calculated risk-takings, and a willingness to tolerate the tentative nature of analytical judgments. These factors are sometimes difficult to achieve in government organizations. Another significant impediment to comprehensive analysis has been a shortage of trained linguists, especially in languages of current interest. As noted above, the

National Security Education Program and related efforts are designed to meet this need, but most observers believe the need for linguists will remain a pressing concern for some years.

An enduring concern is the existence of "stovepipes." Agencies that obtain highly sensitive information are reluctant to share it throughout the intelligence community out of a determination to protect their sources. In addition, information not available to analysts with relevant responsibilities is many times wasted. In recent years there have been calls for greater information sharing in order to improve the quality of analysis and intelligence professionals argue that many problems existing prior to 9/11 have been successfully addressed, but it is expected that dealing with this complex dilemma will require continuing attention by intelligence managers. The unauthorized release of classified documents in 2010 by major newspapers and the Wikileaks website underscored, however, the risks of widespread dissemination of sensitive information.

The Intelligence Community and Iraq and Afghanistan

The successful war on the Taliban regime in Afghanistan in the aftermath of the 9/11 attacks reflected close coordination among CIA paramilitary personnel, DOD Special Forces, and Afghan fighters, mostly from the Northern Alliance that had long been engaged in hostilities with the Kabul government. It combined careful gathering of targeting information, precision strikes by U.S. aircraft, and effective partnership with Afghan leaders. CIA personnel entered Afghanistan in later September 2001 and by December the Taliban had been removed from power. Although establishing a new Afghan government was challenging, the campaign (Operation Enduring Freedom) demonstrated the value of the extensive ties that the CIA had maintained with Afghanis after the common struggle against the Soviet occupation in the 1980s, as well as effective coordination with DOD Special Forces, and with military commanders.

Although intelligence support contributed significantly to the success of Operation Iraqi Freedom and the fall of the Saddam regime in April 2003, the intelligence community was widely criticized for its performance in regard to the aftermath of victory. The Baath Government in Bagdad undeniably presented major challenges; it was almost impossible to penetrate the inner reaches of Saddam Hussein's government. U.S. intelligence agencies supported the efforts of U.N. inspectors charged with determining Iraqi compliance with U.N. resolutions requiring Iraq to end any programs for the acquisition or deployment of weapons of mass destruction, but such efforts were frustrated by the Iraqi government.

At Congress's request, a National Intelligence Estimate (NIE) dealing with Iraqi weapons of mass destruction (WMD) was prepared in September 2002, shortly before crucial votes on the Iraqi situation. The NIE has been widely criticized for inaccurately claiming the existence of actual WMDs and exaggerating the extent of Iraqi WMD programs. The Senate Intelligence Committee concluded that the NIE's major key judgments "either overstated, or were not supported by, the underlying intelligence reporting."

Other observers note, however, that the intelligence community based its conclusions in significant part on Iraq's previous use of WMD, its ongoing WMD research programs, and its unwillingness to document the destruction of WMD stocks in accordance with U.N. resolutions. These factors served as background to Administration decisions. Some observers argue, however,

that Administration officials misused intelligence in an effort to build support for a military option.[4]

On February 11, 2004, President Bush by Executive Order 13328 created a Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. The commission, co-chaired by former Senator Charles S. Robb and retired Federal Judge Laurence H. Silverman, was asked to assess the capabilities of the intelligence community to collect, analyze, and disseminate intelligence regarding WMD and related 21st century threats. In addition, the commission was asked to look specifically at intelligence regarding Iraqi WMD prior to Operation Iraqi Freedom and to compare prewar assessments with the findings of the Iraq Survey Group. The commission issued its report on March 31, 2005.[5] The report described in detail a number of analytical errors that resulted in faulty pre-war judgments on Iraq's weapons of mass destruction. The commission recommended that the DNI take steps to forge an integrated intelligence community, that intelligence functions within the FBI be combined into a single National Security Service, and urged that the DNI not focus on the preparation of the President's Daily Brief at the expense of the long-term needs of the intelligence community.

Despite the inadequate intelligence on Iraqi WMD programs, the success of the military attack on the Iraqi regime launched in March 2003 by the United States, the UK, and other countries was greatly assisted by intelligence. The extensive use of precision-guided munitions that targeted key Iraqi military and command facilities and limited civilian casualties was made possible by the real-time availability of precise locating data. Observers have noted that operational shortcomings in transmitting intelligence data that were frequent during the 1991 Persian Gulf War were not observed in the Iraq campaign of 2003.

The intelligence community did not predict the extent of communal infighting in post-invasion Iraq and was hard pressed to support US and Allied military forces subject to attacks by both Sunni and Shia elements during the three years after the collapse of Saddam Hussein's regime. Conditions in Iraq improved considerably beginning in 2007 after the "Surge," under the leadership of General David Petraeus, along with initiatives of the Iraqi government. The Surge depended on intensified efforts to achieve "situational awareness" as a component of its effort to locate terrorists and provide security to the Iraqi population. This awareness was achieved by the military's operating forces with significant support from intelligence agencies.

Campaigns in both Iraq and Afghanistan demonstrated the importance of intelligence provided by unmanned aerial systems and other tactical ISR systems. Secretary of Defense Robert Gates underscored the importance of this role when he proposed additional funding for ISR in his FY2010 budget request. Operations in Afghanistan which have intensified as U.S. forces are being reduced in Iraq are based on greater capabilities at achieving situational awareness with a special focus on avoiding civilian casualties. The need for additional funding for tactical ISR systems for Afghan operations was reflected in DOD budget submissions for FY2010 and in reprogramming actions. In general, requests for additional ISR resources were incorporated in subsequent defense authorization and appropriation acts. Many of the increments were included in the FY2011 budget submissions and ultimately in defense authorization legislation (H.R. 6523) that was signed by the President on January 7, 2011, becoming P.L. 111-383.

[4] For additional background, see CRS Report RS21696, *U.S. Intelligence and Policymaking: The Iraq Experience*, by Richard A. Best Jr.

[5] The report may be found at http://www.gpoaccess.gov/wmd/index.html.

Senior U.S. commanders in Afghanistan have argued that intelligence resources should be directed not only at identifying enemy fighters but also at providing better situational awareness of the local conditions—governance, development, and local populations—to assist in improving stability operations.

International Terrorism

Although intelligence agencies were focused on international terrorism from at least the mid-1980s, the events of September 11, 2001, made counterterrorism a primary mission of the intelligence community. In response to a widespread perception that statutory barriers restricted the flow of information between the CIA and the FBI, Congress passed the USA PATRIOT Act (P.L. 107-56) which removed impediments to sharing foreign intelligence and law enforcement information (including grand jury information). The PATRIOT Act was designed to facilitate an all-source intelligence effort against terrorist groups that work both inside and outside U.S. borders. Nevertheless, problems of coordination and institutional rivalries persist. Some provisions in the USA PATRIOT Act relating to the sharing of law enforcement and foreign intelligence information were to have expired in early 2006, but new legislation (P.L. 109-177 and P.L. 109-178) extended expiring provisions with modifications. In February 2010 Congress further extended certain provisions of the USA Patriot Act for an additional 12 months.

The Department of Homeland Security, established in 2003, contains an analytical office responsible for integrating information from foreign intelligence and law enforcement sources. In addition, the Bush Administration announced the establishment of the Terrorist Threat Integration Center (TTIC) in January 2003 under the DCI. In accordance with EO13354 of August 27, 2004, and the Intelligence Reform Act, TTIC was transferred to the National Counterterrorism Center (NCTC) and constitutes the focal point for assessing information on potential terrorist threats from all sources.[6] Congress is reviewing the performance of the NCTC in the aftermath of the December 25, 2009, plot against an American airliner.

As an intelligence mission, counterterrorism has several unique characteristics. Although it usually requires input from all the various intelligence disciplines, most observers believe that it is especially dependent upon *humint*. Technical systems are good at providing information about numbers of airplanes, ships, and tanks but the most important information on small groups of terrorist plotters often is provided by human sources. Furthermore, the type of humint required for counterterrorism depends on contacts with sources far removed from embassy gatherings and requires expertise in languages that are possessed by few in this country. This is a distinct difference from humint collection during the Cold War when Soviet diplomats and military officers were often the principal targets.

Intelligence Support to Military Forces

In 1997, the House Intelligence Committee noted that "intelligence is now incorporated into the very fiber of tactical military operational activities, whether forces are being utilized to conduct humanitarian missions or are engaged in full-scale combat." The Persian Gulf War demonstrated the importance of intelligence from both tactical and national systems, including satellites that

[6] See CRS Report R41022, *The National Counterterrorism Center (NCTC)—Responsibilities and Potential Congressional Concerns*, by Richard A. Best Jr.

had been previously directed almost entirely at Soviet facilities. There were, nonetheless, numerous technical difficulties, especially in transmitting data in usable formats and in a timely manner. Many of these issues have since been addressed with congressional support and in Operation Iraqi Freedom intelligence was an integral part of the operational campaign and remain so in operations in both Iraq and Afghanistan.

Issues in the 112th Congress

Observers expect that oversight of the implementation of the Intelligence Reform Act will extend into the 112th Congress. Congress may also monitor the evolving relationship between the DNI and the CIA Director, especially in regard to humint collection and covert operations as well to CIA's analytical efforts. The roles of the Defense Department and the Under Secretary of Defense for Intelligence may also be congressional concerns. Future satellite procurement programs are an important issue given the multi-billion dollar costs involved, though many of the details remain classified.

Christmas Bombing 2009

Interest in better analysis was bolstered by the Administration's review of the December 25, 2009, attack on Northwest Airlines Flight 253 preparing to land in Detroit. Unlike the situation prior to 9/11, in this case there was reportedly adequate information and it was shared with relevant agencies. According to an executive branch review of incident, "The U.S. government had sufficient information to have uncovered and potentially disrupted the December 25 attack ... but analysts within the CT [counterterrorism] community failed to connect the dots that could have been identified and warned of the specific threat. The preponderance of the intelligence related to this plot was available broadly to the Intelligence Community."[7]

The failed effort raised a number of questions among Members about the effectiveness of the intelligence community's counterterrorism efforts. Some have strongly criticized the Administration for failing to keep the intelligence committees fully and currently informed of the status of the ongoing investigation of the planned attack. On May 18, 2010, SSCI published an unclassified Executive Summary of a *Committee Report on the Attempted Terrorist Attack on Northwest Airlines Flight 253*. The report is strongly critical of the State Department for not revoking the U.S. visa of the suspect, Umar Farouk Abdulmutallab. It also criticizes various intelligence agencies for not collecting and disseminating available information. The review suggested that at the CIA, "Inadequate technological search tools and the fragmented nature of the Intelligence Community's databases made it difficult to find additional information related to Abdulmutallab." Further, the "NCTC was not adequately organized and did not have resources appropriately allocated to fulfill its missions." In addition, "counterterrorism analysts at NCTC, CIA, and NSA were focused on the threat of terrorist attacks in Yemen, but were not focused on the possibility of AQAP [Al-Qaeda in the Arabian Peninsula] attacks against the U.S. homeland."

[7] See White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack, at http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack.

ISR Programs

Although major intelligence, surveillance, and reconnaissance programs are classified and discussed in the classified annexes of intelligence authorization and defense appropriations acts, they include a substantial portion of the overall intelligence budget. Defense Secretary Gates has proposed significant increases in spending for ISR and funding ISR programs in annual defense authorization bills.

Considerable controversy exists over the future direction of satellite acquisition. Although much of the discussion remains classified, according to media accounts there appears to be deep skepticism in the Senate Intelligence Committee in regard to administration proposals for a new generation of electro-optical satellites. Initiatives in DOD to acquire satellites for use of tactical commanders appear to some observers as insufficiently coordinated with programs to acquire satellites for national-level agencies, raising the potential of waste and duplication of effort. Also at issue is the appropriate extent of increased purchases of imagery from commercial vendors. All acknowledge that commercial imagery makes an important contribution to government agencies, but some argue that commercial products may not be able to meet government requirements as the commercial market evolves.

Terrorist Surveillance Program/NSA Electronic Surveillance/FISA

In December 2005 media accounts of electronic surveillance by NSA authorized outside the parameters of the Foreign Intelligence Surveillance Act (FISA) led to extensive criticism of the Administration. Although the technical details of the effort remain classified, the Bush Administration maintained that communications, which involve a party reasonably considered to be a member of Al Qaeda, or affiliated with Al Qaeda, and one party in the United States, may be monitored on the basis of the President's constitutional authorities and the provisions of the Joint Resolution providing for Authority for the Use of Force (P.L. 107-40) of September 18, 2001. The need for speed and agility required, the Administration further argued, an approach not envisioned by the drafters of FISA. Others countered that FISA should have governed such electronic surveillance. In early March 2006 agreement was reached with the leadership of the two intelligence committees to establish procedures for enhanced legislative oversight of the NSA effort, and legislative initiatives were considered to either modify FISA or establish new statutory authorities for electronic surveillance.

Differing views of Members on the NSA effort were reflected in the House Intelligence Committee's 2006 report on FY2007 intelligence authorization legislation (H.Rept. 109-411).[8] In light of decisions issued by the Foreign Intelligence Surveillance Court (FISC) on January 10, 2007, the Bush Administration advised the chairman and ranking Member of the Senate Judiciary Committee that any electronic surveillance that had previously occurred as part of the Terrorist Surveillance Program (TSP) would thereafter be conducted subject to the approval of the FISC. Further, the Administration indicated that it would not re-authorize the TSP after the expiration of the then-current authorization. On May 1, 2007, the Senate Intelligence Committee held an open hearing on the Administration's proposal to revise FISA to take account of changes in

[8] See also CRS Report RL33637, *Electronic Surveillance Modernization Act, as Passed by the House of Representatives*, by Elizabeth B. Bazan, and CRS Report RL33669, *Terrorist Surveillance Act of 2006: S. 3931 and Title II of S. 3929, the Terrorist Tracking, Identification, and Prosecution Act of 2006*, by Elizabeth B. Bazan.

communications technologies since the 1970s, with Members expressing differing views on the desirability of the legislation.[9]

According to media reports, a judge on the FISC at some point in 2007 ruled that a FISC order was required for surveillance of communications between foreign persons abroad if the communications passed through the United States. On August 2, 2007, the DNI issued a statement on FISA modernization in which he contended that the intelligence community "should not be required to obtain court orders to effectively collect foreign intelligence from foreign targets located overseas." Although details of the effort remain classified, there appears to have been wide agreement among Members that FISA needed to be amended to permit surveillance without a court order of such foreign to foreign communications regardless of whether they were routed through the United States.

The Protect America Act (PAA) (P.L. 110-55), signed on August 5, 2007, after extensive congressional debate, excluded from the definition of "electronic surveillance" under FISA surveillance directed at a person reasonably believed to be located outside the United States. In addition, under certain circumstances, FISA, as amended by this legislation, permitted the DNI and the Attorney General, for periods up to one year, to authorize acquisition of foreign intelligence information "concerning persons reasonably believed to be located outside of the United States," apparently including U.S. persons, and to direct a communications provider, custodian, or other person with access to the communication immediately to provide information, facilities, and assistance to accomplish the acquisition. Those receiving such directives had the right to contest them in court. The DNI and the Attorney General were required to certify, in part, that this acquisition did not constitute electronic surveillance; and the Attorney General was required to submit the procedures by which this determination is made to the FISC for review as to whether the government determination was clearly erroneous. On a semiannual basis, the Attorney General was to report to congressional oversight committees on instances of noncompliance with directives and numbers of certifications and directives issued during the reporting period. P.L. 110-55 expired on February 1, 2008, and efforts to extend it further failed in the House when H.R. 5349 was rejected on February 13. Acquisitions authorized while the PAA was in force may continue until the expiration of the period for which they were authorized.

The Protect America Act was strongly criticized by some Members; on November 15, 2007, H.R. 3773, the RESTORE Act (the Responsible Electronic Surveillance that is Overseen, Reviewed, and Effective Act of 2007) was passed by the House to clarify that a court order is not required for the acquisition of the contents of communications between two persons neither of whom is known to be a U.S. person, and both of whom are reasonably believed to be located outside the United States, regardless of whether the communications passed through the United States or if the surveillance device was in the United States. If, in the course of such an acquisition, the communications of a U.S. person were incidentally intercepted, stringent minimization procedures would apply. Court orders would, however, be required if the communications of a non-U.S. person reasonably believed to be located outside the United States were targeted where the other parties to the target's communications are unknown and thus might include U.S. persons or persons located physically in the United States. Some Members argued that this provision would unnecessarily tie the hands of intelligence agencies and jeopardize the counterterrorism effort. The RESTORE Act would have also provided for increased judicial oversight and would

[9] See CRS Report RL34279, *The Foreign Intelligence Surveillance Act (FISA): An Overview of Selected Issues*, by Elizabeth B. Bazan.

have required quarterly implementation and compliance audits by the Inspector General of the Justice Department, and added related congressional reporting requirements.

On October 26, 2007, the Senate Intelligence Committee reported its own version of a FISA amendment. The Senate bill (S. 2248), as amended, contained provisions authorizing the Attorney General and the DNI jointly to authorize targeting of persons, other than U.S. persons, reasonably believed to be outside the United States to acquire foreign intelligence information for periods up to one year. Under the Senate bill, FISC approval would be required for targeting a U.S. person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance under FISA, or the acquisition of stored electronic communications or stored electronic data that requires an order under FISA, and the acquisition is conducted in the United States. The Senate bill also provided some retroactive immunity to telecommunications companies from civil suits in federal and states courts related to assistance that they have provided to the government in connection with intelligence activities between September 11, 2001, and January 17, 2007.

A central issue was the role of the judicial branch, and the FISC in particular, in approving and/or overseeing surveillance that does not target but may involve individuals who are U.S. persons. Some argued that only the independent judiciary could ensure that intelligence efforts would not become improperly or illegally directed towards Americans. At the time FISA permitted electronic surveillance to gather foreign intelligence information pursuant to a FISC order of U.S. persons where there was probable cause to believe they were foreign powers or agents of foreign powers if other statutory criteria were met. Some argued, however, that changes in technologies since FISA was enacted in 1978 made case-by-case judicial review of each international communication link that might involve a U.S. person impractical and risky to national security. Details of this issue are complex and, in many cases, classified. The Senate approved S. 2248 on February 12, 2008 (and incorporated it into H.R. 3773).

On March 14, 2008, the House approved an amendment to the version of H.R. 3773 that had been approved by the Senate. The House amendment would have required judicial review by the FISC of procedures for targeting a non-U.S. person located outside of the United States even if the person was not reasonably believed to be communicating with a U.S. person or a person in the United States. The House amendment would require either a prior FISC order approving the applicable certification, targeting procedures, and minimization procedures or a determination that an emergency situation exists in which case a certification would have to be filed with the FISC within seven days. The Bush Administration argued that this requirement added unprecedented requirements for targeting communications of non-U.S. persons that could result in delaying collection efforts and the loss of some intelligence forever.

If the target of an acquisition were a U.S. person reasonably believed to be outside the United States, then, except in emergencies, the House-passed amendment would have required a FISC order approving an application for an acquisition for a period up to 90 days. The acquisition could have been renewed for additional 90 day periods upon submission of renewal applications. If the Attorney General authorized an emergency acquisition of such a U.S. person's communications, the Attorney General would have had to submit an application for a court order within seven days of that authorization.

The House version of H.R. 3773 would also not have granted retroactive immunity to telecommunications companies but would have allowed them to present evidence in their defense to a court. In addition, the House bill would have established a commission on warrantless

electronic surveillance activities conducted between September 11, 2001, and January 17, 2007. The House version of H.R. 3773 did not come to a vote in the Senate and, after considerable discussions, Representative Reyes introduced a new bill, H.R. 6304, on June 19 that strengthened the role of the FISC in approving procedures for intelligence surveillance and provided telecommunications companies an opportunity to demonstrate to the courts that they had acted in response to a request for support from the executive branch. H.R. 6304 was passed by the House on June 20, 2008, and by the Senate on July 9, 2008; it was signed by the President on July 10, becoming P.L. 110-261.

At the end of 2009 three FISA provisions, dealing with "Lone Wolf" terrorists, roving wiretaps, and access to business records, were set to expire unless extended.[10] They were extended until February 28, 2010, by a provision of the Defense Appropriations Act for FY2010 (P.L. 111-118) and separate legislation (P.L. 111-141) extended them until February 28, 2011.

Role of the CIA

Intelligence reform legislation enacted in 2004 is having a significant effect on the work of the CIA. The CIA Director does not have the community-wide responsibilities that historically absorbed the attention of the DCI, nor is he responsible for daily morning briefings in the White House. In his role as National Humint Manager, the CIA Director oversees the National Clandestine Service's efforts humint collection by the CIA and coordinates humint efforts by other agencies. The CIA also retains primary responsibilities for all-source analysis on a vast array of international issues that are of concern to the U.S. government. Some observers suggest that the CIA has lost stature as a result of the Intelligence Reform Act that placed the DNI between the head of the CIA and the President. Other observers argue, however, that without the burden of interagency coordination, the CIA Director is better positioned to emphasize analytical and humint collection activities. Congress has expressed concern about both humint and the conduct of analysis on repeated occasions and may choose to oversee the CIA Director's efforts more closely.

Role of the FBI

In the wake of the September 2001 attacks, the FBI was strongly criticized for failing to focus on the terrorist threat, for failing to collect and strategically analyze intelligence, and for failing to share intelligence with other intelligence agencies (as well as among various FBI components). Subsequently, FBI Director Robert S. Mueller III introduced a number of reforms to create a better and more professional intelligence effort in an agency that has always emphasized law enforcement. Congress has expressed concern about the overall effectiveness of these reforms and with the FBI's widely criticized information technology acquisition efforts.[11]

[10] See CRS Report RL34566, *The Foreign Intelligence Surveillance Act (FISA): A Sketch of Selected Issues*, by Elizabeth B. Bazan. See also CRS Report R40138, *Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire February 28, 2011*, by Edward C. Liu.

[11] For further information, see CRS Report RL33033, *Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress*, by Alfred Cumming.

The Role of the Under Secretary of Defense for Intelligence

The position of Under Secretary of Defense for Intelligence (USD(I)) was established by the Defense Authorization Act for FY2003 (P.L. 107-314, sec. 901). The statute and DOD directives give the incumbent significant authorities for the direction and control of intelligence agencies within DOD especially in regard to systems acquisition. There are reports that DOD special forces have also been involved in human intelligence collection efforts that are not effectively coordinated with CIA. Some media commentators have pointed to potential conflicts between the office of the USD(I) and the DNI's office, but there is little official information available publicly. The first USD(I), Stephen Cambone, resigned at the end of 2006; his successor was retired Air Force Lt. General James Clapper, who previously served as director of both NGA and DIA and who would become DNI in August 2010. In May 2007 the USD(I) was also designated Director of Defense Intelligence and also serves on the DNI's executive committee.

Paramilitary Operations and Defense Humint

Some observers have expressed concern that expanded efforts by DOD intelligence personnel to collect humint overseas and undertake "preparation of the battlefield" operations may interfere with ongoing efforts of CIA humint collectors. Intelligence officials have maintained in congressional testimony that there is no unnecessary duplication of effort and that careful coordination is undertaken during the planning and implementing of such operations. The determination to ensure that such coordination is effective was further reflected in the designation of the DCIA as head of the National Clandestine Service.

Regional Concerns

Despite the urgency of the counterterrorism mission, the intelligence community is responsible for supporting traditional national security concerns, including developments in China, North Korea, Iran, and South America. These collection and analytical efforts require considerable investments in collection systems and the development of analytical expertise extending over many years.

CIA and Allegations of Prisoner Abuse

Media accounts of abuse of prisoners by CIA officials or contractors have led to calls for a congressional investigation. Some have also raised broader concerns about the role of intelligence agencies in holding and transporting prisoners. The conference version of the FY2008 Intelligence Authorization bill (sec. 327) included provisions requiring all executive branch agencies, including the CIA, to use only interrogation techniques authorized by the Army Field Manual. Opposition to this provision was a primary reason cited in President Bush's message vetoing this legislation on March 8, 2008. Upon taking office, President Obama directed that the Army Field Manual be used by all U.S. agencies (except the FBI which has its own approved procedures). Some Members have introduced legislation to establish statutory restrictions on interrogation techniques.[12]

[12] See CRS Report R40754, *Guantanamo Detention Center: Legislative Activity in the 111th Congress*, by Michael John Garcia.

In early March 2009, the leadership of the Senate Intelligence Committee announced that the committee will review CIA's detention and interrogation activities subsequent to 9/11 in an attempt to shape future policies. In April 2009, the Administration released copies of memoranda that authorized specific interrogation techniques. Completion of the review has not been announced.

Congressional Notification Procedures

The intelligence investigations of the 1970s led to eventual enactment of statutory provisions requiring that Congress be informed of covert actions as well as current and anticipated intelligence activities other than covert actions. These provisions require the Administration to keep the two intelligence committees "fully and currently informed" of intelligence activities and significant anticipated intelligence activities. Covert actions must be approved by the President and Congress must be notified, but special provisions were subsequently established to permit in extraordinary circumstances limiting notification of covert actions to the chairmen and ranking minority Members of the intelligence committees, the Speaker of the House and the House minority leader, and the majority and minority leaders of the Senate, the so-called "Gang of Eight." Whether Gang of Eight or even more limited notification can be used for intelligence activities other than covert actions has become a source of controversy in recent years with some Members arguing that the statutes require that all committee Members be notified at least in the case of intelligence activities that are not covert actions. The House Intelligence Committee included a provision (Section 321) in its FY2010 intelligence authorization bill (H.R. 2701) that would remove the Gang of Eight provisions and require that all committee Members be briefed on all intelligence activities, including covert actions, unless the committee itself decided to limit notification. The Administration, in its Statement of Administration Policy issued July 8, 2009, stated firm opposition to Section 321, arguing that it "runs afoul of tradition by restricting an important established means by which the President protects the most sensitive intelligence activities."[13] The Senate version of the FY2010 intelligence authorization bill, which ultimately became P.L. 111-259, addresses notification both of covert actions and intelligence activities generally; it would require that, if the Administration does not provide information to all Members of the two committees, it will be required to notify the committees of the reasons for withholding information and a description of the "main features" of the activity that can be made available to all committee Members.

Civilian Intelligence Personnel System

Changes in personnel regulations for intelligence personnel, including the Defense Civilian Intelligence Personnel System (DCIPS), which introduced "pay bands" in which the pay of civil servants could be adjusted on the basis of performance assessments, have been criticized for lacking transparency and having the potential for abuse. The goal was to link pay and performance, but critics have argued that the system has the potential for abuse and an adverse effect on minorities. Section 1114 of the FY2010 Defense Authorization Act (P.L. 111-84) required that basic pay of civilian employees of intelligence agencies not be fixed under the Defense Civilian Intelligence Personnel System pending reviews by the Government Accountability Office and an independent organization. On August 4, 2010, DOD announced that

[13] CRS Report R40691, *Sensitive Covert Action Notifications: Oversight Options for Congress*, by Alfred Cumming; also CRS Report R40698, *"Gang of Four" Congressional Intelligence Notifications*, by Alfred Cumming.

it would not implement DCIPS policies (other than those at the NGA that had long had a system similar to DCIPS) and would return to a General Schedule-like pay system.

Government Accountability Office and the Intelligence Community

The Government Accountability Office (GAO), a legislative branch agency, has statutory authorities to audit and investigate the receipt, disbursement, and application of public funds with a broad right of access to agency records and information. There are, however, specific exceptions that cover many intelligence activities by the CIA and other intelligence agencies. Although oversight of intelligence efforts is undertaken by the two congressional intelligence agencies, some Members believe that the GAO should also have a role in intelligence efforts.[14] In recent years, intelligence authorization bills have included provisions expanding GAO's responsibilities in regard to intelligence agencies; both the Bush and Obama Administrations have resisted these proposals. Provisions for an expanded GAO role were included in both the Senate and House FY2011 Intelligence Authorization bill (S. 1494, Section 335; H.R. 2701, Section 335) despite Administration opposition.[15] On May 27, 2010, an amendment sponsored by Representative Eshoo was added to the FY2011 Defense Authorization bill (H.R. 5136, Section 923) on a floor vote that would require the DNI to provide the GAO with all information necessary to conduct an analysis, evaluation, or investigation requested by one of the congressional intelligence committees. In addition, a separate section would recognize that GAO audits of intelligence agencies could be requested by any congressional committee with appropriate jurisdiction. In such cases, information relating to intelligence sources and methods or covert actions may be redacted and provided only to the congressional intelligence committees. The version of H.R. 2701 that both the Senate and House approved in late September 2010 requires that the DNI issue a written directive no later than May 2011 to govern access by GAO for information held by intelligence agencies. The directive is to take effect 60 days after it is submitted to Congress.

109th Congress Legislation

H.R. 2475 (Hoekstra)
Intelligence Authorization Act for FY2006; introduced May 19, 2005; reported June 2, 2005 (H.Rept. 109-101); passed House June 21, 2005.

H.R. 5020 (Hoekstra)
Intelligence Authorization Act for FY2007; introduced March 28, 2006; reported April 6, 2006 (H.Rept. 109-411); passed House April 26, 2006.

[14] See CRS Report RL32525, *Congressional Oversight of Intelligence: Current Structure and Alternatives*, by Frederick M. Kaiser, "GAO Versus the CIA: Uphill Battles Against an Overpowering Force," *International Journal of Intelligence and Counterintelligence*, Fall 2002. Similar proposals have been introduced over a long period, including stand-alone legislation such as S. 385, introduced by Senator Daniel Akaka in the 111th Congress, S. 82, in the 110th congress also introduced by Senator Akaka, and H.R. 978 introduced by Representative Bennie Thompson, and H.R. 3603 in the 100th Congress, introduced by then-Representative Leon Panetta.

[15] Office of Management and Budget, Statement of Administration Policy, H.R. 2701, Intelligence Authorization Act for Fiscal Year 2010, July 8, 2009.

S. 1803 (Roberts)
Intelligence Authorization Act for FY2006; introduced and reported by the Select Committee on Intelligence, September 29, 2005 (S.Rept. 109-142); reported by the Armed Services Committee, October 27, 2005 (S.Rept. 109-173).

S. 3237 (Roberts)
Intelligence Authorization Act for FY2007; introduced and reported by the Select Committee on Intelligence, May 25, 2006 (S.Rept. 109-259); reported by the Armed Services Committee, June 21, 2006 (S.Rept. 109-265).

110th Congress Legislation

S. 372 (Rockefeller)
Intelligence Authorization Act for 2007. Introduced and reported by the Select Committee on Intelligence, January 24, 2007 (S.Rept. 110-2). Debated April 16-17, 2007.

S. 1538 (Rockefeller)
Intelligence Authorization Act for 2008. Introduced and reported by Select Committee on Intelligence, May 31, 2007 (S.Rept. 110-75). Reported by Armed Services Committee, June 26, 2007 (S.Rept. 110-92). Floor consideration, October 3, 2007; incorporated into H.R. 2082 as an amendment.

H.R. 1196 (Reyes)
Intelligence Authorization Act for FY2007. Introduced and referred to the Permanent Select Committee on Intelligence, February 27, 2007.

H.R. 2082 (Reyes)
Intelligence Authorization Act for FY2008. Introduced and referred to the Permanent Select Committee on Intelligence, May 1, 2007 (H.Rept. 110-131). Reported, May 2, 2007; debated May 10-11, 2007; approved May 11, 2007. Conference report (H.Rept. 110-478) filed December 6. House approved conference report, December 13, 2007; Senate approved conference report, February 13, 2008. Returned (vetoed) by the President, March 8, 2008.

H.R. 5959 (Reyes)
Intelligence Authorization Act for FY2009. Introduced and referred to Permanent Select Committee on Intelligence, May 5, 2008. Reported (amended), May 21, 2008.

S. 2996 (Rockefeller)
Intelligence Authorization Act for FY2009. Original measure reported, May 8, 2008.

111th Congress Legislation

H.R. 2701 (Reyes)
Intelligence Authorization Act for FY2010. Introduced and referred to the Permanent Select Committee on Intelligence, June 4, 2009. Reported, June 26, 2009 (H.Rept. 111-186). Passed, amended, February 26, 2010. Passed Senate, amended, September 27, 2010. Senate amendment passed House, September 29, 2010. Signed by the President, October 7, 2010. P.L. 111-259.

H.R. 5161 (Reyes)
Intelligence Authorization Act for FY2011. Introduced and referred to the Permanent Select Committee on Intelligence, April 28, 2010.

S. 1494 (Feinstein)
Intelligence Authorization Act for FY2010. Original measure reported to the Senate, July 22, 2009 (S.Rept. 111-55). Passed, amended, September 16, 2009.

S. 3611 (Feinstein)
Intelligence Authorization Act for FY2010. Original measure reported to the Senate, July 19, 2010 (S.Rept. 111-223). Passed Senate, August 5, 2010.

112th Congress Legislation

H.R. 754 (Rogers)
Intelligence Authorization Act for FY2011. Introduced and referred to the Permanent Select Committee on Intelligence, February 17, 2011.

For Additional Reading

U.S. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005.

U.S. Congress. Committee of Conference Intelligence Authorization Act for Fiscal Year 2005: Conference Report. December 7, 2004. 108th Congress, 2nd session (H.Rept. 108-798).

——. *Intelligence Reform and Terrorism Prevention Act of 2004*. December 7, 2004. 108th Congress, 2nd session. (H.Rept. 108-796).

U.S. Congress. House of Representatives. Permanent Select Committee on Intelligence. Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*. December 2002. 107th Congress, 2nd session (H.Rept. 107-792). [Also, S.Rept. 107-351]

——. *Intelligence Authorization Act for Fiscal Year 2005*. June 21, 2004. 108th Congress, 2nd session (H.Rept. 108-558).

——. *Intelligence Authorization Act for Fiscal Year 2006*. June 2, 2005. 109th Congress, 1st session (H.Rept. 109-101).

——. *Intelligence Authorization Act for Fiscal Year 2007*. April 6, 2006. 109th Congress, 2nd session (H.Rept. 109-411).

——. *Intelligence Authorization Act for Fiscal Year 2008*. May 7, 2007. 110th Congress, 1st session (H.Rept. 110-131).

——. *Intelligence Authorization Act for Fiscal Year 2008*. Conference Report. December 6, 2007. 110th Congress, 1st session (H.Rept. 110-478).

——. *Intelligence Authorization Act for Fiscal Year 2009*. May 21, 2008. 110th Congress, 2nd session (H.Rept. 110-665).

——. *Intelligence Authorization Act for Fiscal Year 2010*. June 26, 2009. 111th Congress, 1st session (H.Rept. 111-186).

——. Subcommittee on Terrorism and Homeland Security. *Counterterrorism Intelligence Capabilities and Performance Prior to 9-11*. July 2002.

U.S. Congress. Senate. Select Committee on Intelligence. *Report of the Select Committee on Intelligence on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*. July 9, 2004. 108th Congress, 2nd session (S.Rept. 108-301).

——. *Intelligence Authorization Act for Fiscal Year 2006*. September 29, 2005. 109th Congress, 1st session (S.Rept. 109-142).

——. *To authorize Appropriations for Fiscal Year 2005 for Intelligence and Intelligence-Related Activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System*. May 5, 2004. 108th Congress, 2nd session (S.Rept. 108-258).

——. *Intelligence Authorization Act for Fiscal Year 2007*. January 24, 2007. 110th Congress, 1st session (S.Rept. 110-2).

——. *Intelligence Authorization Act for Fiscal Year 2008*. May 31, 2007. 110th Congress, 1st session (S.Rept. 110-75).

——. *Intelligence Authorization Act for Fiscal Year 2009*. May 8, 2008, 110th Congress, 2nd session (S.Rept. 110-333).

——. *Intelligence Authorization Act for Fiscal Year 2010*. July 22, 2009 [S.1494]. 111th Congress, 1st session (S.Rept. 111-55).

——. *Intelligence Authorization Act for Fiscal Year 2010*. July 19, 2010 [S.3611]. 111th Congress, 2nd session (S.Rept. 111-223).

——. *Unclassified Executive Summary of the Committee Report on the Attempted Terrorist Attack on Northwest Airlines Flight 253*. May 18, 2010.

U.S. Department of Justice, Commission for Review of FBI Security Programs, *A Review of FBI Security Programs*, March 2002.

U.S. National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*, July 2004.

Author Contact Information

Richard A. Best Jr.
Specialist in National Defense
rbest@crs.loc.gov, 7-7607